EB10-P-01.013



MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDANTE DO EXÉRCITO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO EXÉRCITO BRASILEIRO

1ª Edição
2024

EB10-P-01.013



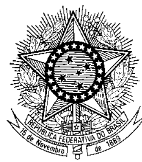
MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDANTE DO EXÉRCITO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO EXÉRCITO BRASILEIRO

1ª Edição
2024



MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COMANDANTE DO EXÉRCITO

PORTARIA – C Ex Nº 2.280, DE 1º DE AGOSTO DE 2024

EB: 64535.051341/2023-92

Aprova a Política de Segurança da Informação do Exército Brasileiro (EB10-P-01.013), 1ª edição, 2024.

O COMANDANTE DO EXÉRCITO, no uso das atribuições que lhe conferem o art. 4º da Lei Complementar nº 97, de 9 de junho de 1999, e o art. 20, inciso XIV, do Anexo I, do Decreto nº 5.751, de 12 de abril de 2006, e considerando o que consta nos autos nº 64535.005164/2023-72, resolve:

Art. 1º Fica aprovada a Política de Segurança da Informação do Exército Brasileiro (EB10-P-01.013), 1ª edição, que com esta baixa.

Art. 2º Fica determinado que o Órgão de Direção Geral, o Órgão de Direção Operacional, os órgãos de direção setorial, os comandos militares de área e os órgãos de assistência direta e imediata ao Comandante do Exército adotem, em suas áreas de competência, as providências decorrentes.

Art. 3º Ficam revogadas as seguintes Portarias:

I - Portaria – C Ex nº 820, de 7 de junho de 2019, que recria o Comitê de Segurança da Informação e Comunicações do Exército Brasileiro e designa o Gestor de Segurança da Informação e Comunicações do Exército Brasileiro; e

II - Portaria – C Ex nº 853, de 12 de junho de 2019, que aprova o Regulamento do Comitê de Segurança da Informação e Comunicações do Exército Brasileiro (EB10-R-01.010), 2ª edição, 2019.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.



FOLHA REGISTRO DE MODIFICAÇÕES (FRM)

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA

ÍNDICE DE ASSUNTOS

Art.

CAPÍTULO I - DAS DISPOSIÇÕES PRELIMINARES

Seção I - Da Finalidade 1º

Seção II - Do Referencial Normativo..2º

Seção III - Dos Conceitos Básicos 3º

CAPÍTULO II - DAS PREMISSAS..4º

CAPÍTULO III - DOS OBJETIVOS...5º

CAPÍTULO IV - DAS ORIENTAÇÕES GERAIS 6º/16

CAPÍTULO V - DAS DISPOSIÇÕES FINAIS 17/19

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Seção I

Da Finalidade

Art. 1º A Política de Segurança da Informação do Exército Brasileiro (POSIN-EB) tem por finalidade estabelecer objetivos e orientações gerais para o Exército Brasileiro (EB) acerca da condução da governança e da gestão da segurança da informação (SI).

Seção II

Do Referencial Normativo

Art. 2º Constitui documentação básica de referência desta Política:

I - Decreto nº 7.809, de 20 de setembro de 2012 — altera os Decretos nº 5.417, de 13 de abril de 2005, nº 5.751, de 12 de abril de 2006, e nº 6.834, de 30 de abril de 2009, que aprovam as estruturas regimentais e os quadros demonstrativos dos cargos em comissão e das funções gratificadas do Ministério da Defesa, bem como dos Comandos da Marinha, do Exército e da Aeronáutica;

II - Decreto nº 9.637, de 26 de dezembro de 2018 — institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da SI;

III - Decreto nº 11.856, de 26 de dezembro de 2023 — institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança;

IV - Portaria – GSI/PR nº 93, de 18 de outubro de 2021 — aprova o Glossário de Segurança da Informação;

V - Portaria – SGD/MGI nº 852, de 28 de março de 2023 — dispõe sobre o Programa de Privacidade e Segurança da Informação;

VI - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, alterada pela Instrução Normativa – GSI/PR nº 2, de 24 de julho de 2020 — dispõe sobre a estrutura de gestão da SI nos órgãos e nas entidades da Administração Pública Federal (APF);

VII - Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 — dispõe sobre os processos relacionados à gestão de SI nos órgãos e nas entidades da APF;

VIII - Normas Complementares nº 5, 8, 9, 12 e 17 a 21 à Instrução Normativa nº 1 GSI/PR, de 13 de junho de 2008 — dispõem sobre temas diversos no contexto da SI;

IX - Portaria – C Ex nº 1.350, de 29 de agosto de 2019 — aprova a Diretriz Estratégica Organizadora do Sistema de Informação do Exército (EB10-D-01.002);

X - Portaria – C Ex nº 781 – Aces Rto, de 6 de agosto de 2020 — estabelece a Diretriz Estratégica Organizadora do Sistema de Inteligência do Exército;

XI - Portaria – C Ex nº 987, de 18 de setembro de 2020 — institui a Política de Governança do Exército Brasileiro (EB10-P-01.007);

XII - Portaria – C Ex nº 1.545, de 30 de junho de 2021 — aprova a Política de Tecnologia da Informação e Comunicações do Exército (EB10-P-01.000);

XIII - Portaria – C Ex nº 2.145, de 18 de dezembro de 2023 — aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), 2ª edição, 2023;

XIV - Portaria – EME/C Ex nº 707, de 20 de abril de 2022 — aprova a Diretriz Organizadora do Sistema de Informações Organizacionais do Exército (EB20-D-02.016);

XV - Portaria – EME/C Ex nº 903, de 7 de novembro de 2022 — aprova a Diretriz de Gestão de Incidentes Cibernéticos no Âmbito do Exército Brasileiro (EB20-D-01.038);

XVI - Portaria – COTER nº 76, de 9 de julho de 2019 — aprova o Manual de Campanha – Contrainteligência (EB70-MC-10.220); e

XVII - ABNT NBR ISO/IEC 27001 — SI, segurança cibernética e proteção à privacidade — sistemas de gestão da SI — requisitos.

Seção III

Dos Conceitos Básicos

Art. 3º Para os fins desta Política, consideram-se os seguintes conceitos básicos:

I - segurança orgânica: segmento da Contrainteligência que preconiza a adoção de um conjunto de medidas destinado a prevenir e obstruir possíveis ameaças de qualquer natureza dirigidas contra pessoas, dados, informações, materiais, áreas e instalações;

II - SI: consiste no conjunto de ações que objetivam viabilizar e assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a irretratabilidade da informação em todo o seu ciclo de vida;

III - disponibilidade: propriedade pela qual se assegura de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

IV - integridade: propriedade pela qual se assegura de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V - confidencialidade: propriedade pela qual se assegura de que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizada nem credenciada;

VI - autenticidade: propriedade pela qual se assegura de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

VII - irretratabilidade (ou não repúdio): propriedade pela qual se assegura de que o emissor de uma mensagem ou a pessoa que executou determinada transação eletrônica não poderá, posteriormente, negar sua autoria;

VIII - ativo: tudo que tenha valor para a organização, material ou não;

IX - ativo de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

X - sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

XI - Sistema de Informação do Exército (SINFOEx): sistema estratégico que tem como objetivo geral promover a eficiente gestão da informação, com o fim específico de apoiar o processo de tomada de decisão, visando ao preparo e ao emprego da Força Terrestre, bem como ao gerenciamento administrativo da Instituição;

XII - auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade com a consecução dos objetivos;

XIII - tecnologia da informação (TI): é o conjunto de todas as atividades e soluções providas por recursos computacionais que viabilizam a obtenção, o armazenamento, a proteção, o processamento, o acesso, a transmissão, o gerenciamento e o uso da informação;

XIV - gestão de SI: processo que visa integrar atividades de gestão de riscos, gestão de continuidade, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à TI;

XV - gestor de SI: responsável pelas ações de SI no âmbito do EB;

XVI - Sistema de Gestão de Segurança da Informação: estrutura pela qual a gestão de SI planeja, desenvolve, executa e monitora as ações e métodos de SI em consonância com a direção definida pela governança;

XVII - Conselho Superior de Tecnologia da Informação (CONTIEx): órgão de assessoramento superior, de caráter deliberativo, acrescido na Estrutura Regimental do Exército por intermédio do Decreto nº 7.809, de 2012, que se destina a assessorar o Comandante do Exército na formulação da Política de Tecnologia da Informação do Comando do Exército, em conformidade com as diretrizes governamentais, bem como no planejamento, na direção e no controle das ações de TI do Comando do Exército;

XVIII - Comitê de Segurança da Informação (COMSI): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de SI no âmbito do órgão ou entidade da APF;

XIX - gestão de continuidade de negócios em SI: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso essas ameaças se concretizem, fornecendo uma estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

XX - informação: dados processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXI - ciclo de vida da informação: compreende todas as fases pelas quais uma informação passa, englobando procedimentos de obtenção, produção, classificação, transporte, utilização, acesso, armazenamento, distribuição, arquivamento e descarte;

XXII - resiliência: capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre e retornar à normalidade das operações;

XXIII - coordenador de SI: referenciado, na literatura especializada, como *Chief Information Security Officer* (CISO), é o responsável pela ligação entre a governança e a gestão de SI no âmbito do EB, bem como pela integração da SI ao planejamento estratégico do EB;

XXIV - dados organizacionais: consistem em um conjunto de palavras, expressões, números ou símbolos relacionados a uma organização, não referentes a uma pessoa identificada ou identificável, inseridos em registros tangíveis ou intangíveis, os quais, após adequado processamento, convertem-se em informações organizacionais, nos termos da Diretriz Organizadora do Sistema de Informações Organizacionais do Exército; e

XXV - proteção de dados organizacionais: refere-se às políticas, procedimentos e processos implementados para garantir a segurança, privacidade e integridade dos dados organizacionais armazenados e processados por uma organização, preservando-se esses contra o acesso ou a divulgação não autorizada, seu uso indevido, modificação, destruição ou furto.

CAPÍTULO II

DAS PREMISSAS

Art. 4º A POSIN-EB baseia-se nas seguintes premissas:

I - a SI abrange a Segurança e a Defesa Cibernética, bem como a segurança física, a proteção de dados organizacionais e as ações destinadas a assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a irretratabilidade da informação;

II - a SI deve ser observada durante todo o ciclo de vida da informação;

III - a SI permeia todas as áreas de atuação relacionadas à informação, tais como a Inteligência, a Comunicação Social, a TI, o Comando e Controle, a Segurança/Defesa Cibernética, a Governança/Gestão Documental e a Governança Digital, entre outras;

IV - a SI deve ser tratada nos níveis de governança e gestão, não se confundindo com a governança e a gestão de TI;

V - as ações de SI envolvem pessoas, processos e tecnologias, sendo que as pessoas constituem seu elo mais fraco;

VI - a gestão de SI deve ter capilaridade, abrangendo todos os elos da cadeia de comando da Instituição não envolvidos na governança; e

VII - a auditoria de SI deve contribuir para a avaliação dos resultados alcançados, em particular quanto aos aspectos de economicidade, eficiência, eficácia e efetividade, com vista ao aperfeiçoamento de sua governança, devendo ficar a cargo do controle interno da Instituição, a fim de preservar seus atributos de independência, imparcialidade e objetividade.

CAPÍTULO III

DOS OBJETIVOS

Art. 5º A POSIN-EB tem por objetivos:

I - garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade da informação em seus suportes (pessoas, documentos, material, meios de TI, áreas e instalações) pertencentes ou custodiados ao EB;

II - alinhar a governança e a gestão de SI no EB com o referencial normativo da APF;

III - contribuir para o aumento da resiliência do SINFOEx;

IV - orientar os diversos escalões do EB, incluindo as entidades vinculadas, quanto às ações necessárias à implantação da SI no âmbito da Instituição;

V - promover o alinhamento das ações de SI a cargo dos diversos sistemas e áreas do EB;

VI - contribuir para a gestão de riscos de SI da Instituição;

VII - orientar a gestão de continuidade de negócios em SI no âmbito do EB;

VIII - aprimorar o sistema de auditoria de SI;

IX - assegurar a irretratabilidade das ações praticadas pelos responsáveis por sistemas de informação da Instituição;

X - desenvolver e manter em permanente aprimoramento a cultura organizacional de SI em todos os níveis da Instituição;

XI - aprimorar a gestão de recursos humanos (processo seletivo, capacitação, desempenho da função, manutenção na atividade e desligamento) envolvidos no tratamento da informação;

XII - aperfeiçoar processos e atualizar tecnologias no intuito de se obter um ambiente seguro para o trâmite da informação; e

XIII - promover a interação com os demais órgãos da APF, comunidade acadêmica, institutos de pesquisa e infraestruturas críticas por meio da atuação colaborativa.

CAPÍTULO IV

DAS ORIENTAÇÕES GERAIS

Art. 6º O Estado-Maior do Exército (EME) regulará a implementação da presente Política no âmbito do EB, abordando, entre outros aspectos:

I - o Sistema de Gestão de SI do EB, definindo suas instâncias e estruturas internas, os processos nele envolvidos e as interações requeridas;

II - as competências e atribuições das estruturas internas de governança e gestão de SI;

III - os mecanismos e práticas de governança e gestão aplicáveis à Instituição, bem como os responsáveis por sua implementação no âmbito do EB;

IV - o tratamento da informação;

V - a segurança física e do ambiente;

VI - a gestão de ativos, particularmente no tocante ao inventário e mapeamento dos ativos de informação;

VII - a gestão do uso dos recursos de TI e de comunicações regulada por normas específicas que abranjam o acesso à internet, correio eletrônico, *Virtual Private Network*, mídias sociais, computação em nuvem, dispositivos móveis, redes sem fio e *backup*, entre outras áreas;

VIII - a gestão de incidentes cibernéticos;

IX - o controle de acesso (físico e lógico);

X - a gestão de riscos de SI;

XI - a gestão de continuidade de negócios em SI;

XII - a auditoria e conformidade de SI; e

XIII - os recursos criptográficos.

Art. 7º A governança de SI do EB é exercida pelo CONTIEx, o qual é assessorado pelo

Comitê de Segurança da Informação do Exército Brasileiro (COMSI-EB).

Art. 8º O 2º Subchefe (SCh) do EME é o CISO do EB.

Art. 9º A gestão de SI no âmbito do EB constitui atribuição do Departamento de Ciência e Tecnologia, que a exerce por meio do gestor de SI do EB, função privativa de oficial-general integrante do COMSI-EB, bem como por sua respectiva equipe setorial de SI.

Art. 10. O EME regulará, por meio da implementação de normas específicas, a proteção de dados pessoais no âmbito do EB.

Art. 11. O Órgão de Direção Geral, os órgãos de direção setorial, o Órgão de Direção Operacional, os comandos militares de área e os órgãos de assistência direta e imediata ao Comandante do Exército devem designar gestores setoriais de SI e suas respectivas equipes de SI.

Art. 12. Os grandes comandos e as grandes unidades devem designar gestores regionais de SI e suas respectivas equipes de SI.

Art. 13. As organizações militares devem designar gestores locais de SI e suas respectivas equipes locais de SI.

Art. 14. A cultura organizacional de SI deve ser buscada por meio das atividades de sensibilização, conscientização e capacitação planejadas, realizadas e verificadas com a frequência requerida para sua efetiva consolidação.

Art. 15. O funcionamento do COMSI-EB será regulado pelo EME.

Art. 16. A secretaria do COMSI-EB será exercida pelo 2º SCh EME.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 17. As violações de SI estarão sujeitas aos instrumentos apuratórios e, se for o caso, às sanções previstas no arcabouço normativo vigente.

Art. 18. O EME deverá expedir diretriz relativa à SI.

Art. 19. Esta Política deverá ser atualizada a cada quatro anos, ou a qualquer tempo, por iniciativa do EME.